Meeting ADAS SoC Safety Design Challenges with Active Safety Features Built In to IP

Cadence

TSMC 2016
Open Innovation Platform®
Ecosystem Forum

ABSTRACT

The automotive industry is going through a fast-paced electronic revolution, driven by higher and higher demand of autonomous vehicles. New vehicles released to market today are already deploying 6-10 ADAS modules with various sensors capable of supporting high- automation levels defined by NHTSA. However, challenges remain to unleash the power of technology due to safety concerns. Due to high computation demand and support for multiple sensors, ADAS SoC is extremely complex to design and requires bleeding edge process nodes. Semiconductor vendors and Tier-1 suppliers developing ADAS ASICs must rely on IP suppliers to achieve silicon success. IPs designed using traditional safety methodology may achieve the goal of stringent level functional safety standards but are no longer sufficient to meet the real time safety decisions required in current and future ADAS SoCs. In order to design effective functional safety mechanism at SoC level, the internal logic of the ADAS optimized IPs need to incorporate additional functionalities to offload and also complement the complexities in the system design.

Cadence has been working with automotive semiconductor vendors and Tier-1 suppliers to ensure that IPs are meeting functional safety requirements defined by ISO26262 standard. In this process, we are also adding active functional safety mechanisms as differentiating features into the IPs. These features are documented in the functional safety manuals delivered to customers. They are also systematically analyzed in ISO26262 FMEDA report to quantify the effectiveness of the features in reducing undetectable failure rates. In this presentation, we will present the representative functional safety features that have been instrumented in various IPs, their impact to SoC level functional safety architecture, and the ISO26262 FMEDA evaluation process to quantify the effectiveness of these features.

Achieving physical device level reliability is crucial to ensure that the device doesn't enter random failure modes during the long operating life cycle. Cadence hard IPs are designed using the design rules and simulation models to match AEC-Q100 requirements. The IPs are going through AEC-Q100 testing using test chips to bring confidence to our customers the long term reliability of their products.

Meeting ADAS SoC Safety Design Challenges with Active Safety Features Built In to IP

Charles Qi, Sr. Design Engineering Architect
TSMC OIP
San Jose, California
September 2016

cadence

Self-Driving Car: the **Vision** and the **Reality**

Poster at 2015 SAE Congress: Future Self-Driving Car

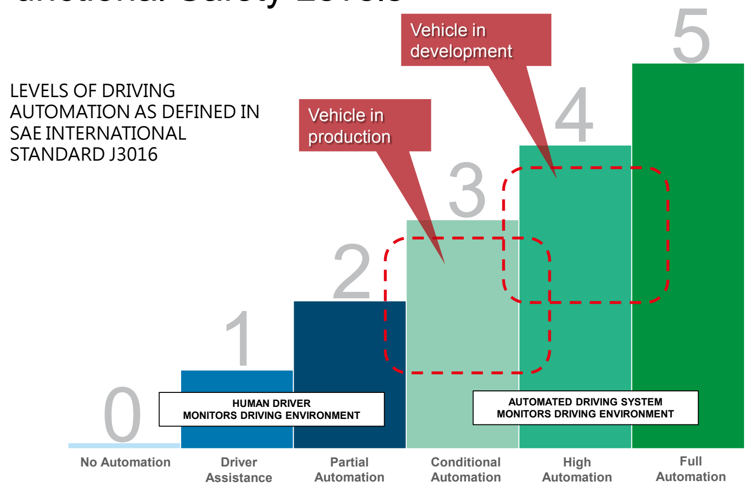
100% machine-controlled, no active driver

Tesla Model S Autopilot Partial ADAS in Production

Over 130 million real road miles, but fatal accident occurs…

cadence

Fully Autonomous Demands Very High Functional Safety Levels



The auto industry has passed Stages 0-2, moving aggressively to Stages 3-5

cadence

Trends in Safety Design for ADAS

Observations based on customer demands

Increased Safety Impact
- Safety is non-optional at levels 4-5 because machines are performing real-time vehicle control
- Safety failure results in fatalities, recalls, and lawsuits
- Vehicle must fail-operational or not fail

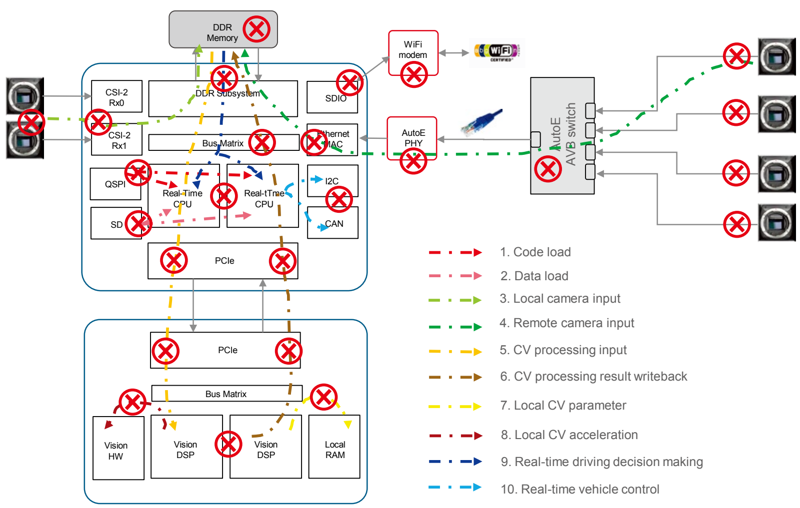
Increased System/SoC Complexity
- High-intelligence design with many vendor participation
- Multi-sensor, multi-processor operation
- Many I/O/network interfaces, memory hierarchies
- Complex interaction of hardware/software components

Safety Is Designed in Early
- No assurance of system safety with blackbox components designed without safety principles
- Localized failures non-detectable by high-level agents
- After-thought protection mechanisms are not fail-operational

cadence

Safety Design Challenges in Complex ADAS SoCs

Complex data flow, many failing points in ADAS chip-set



  cādence

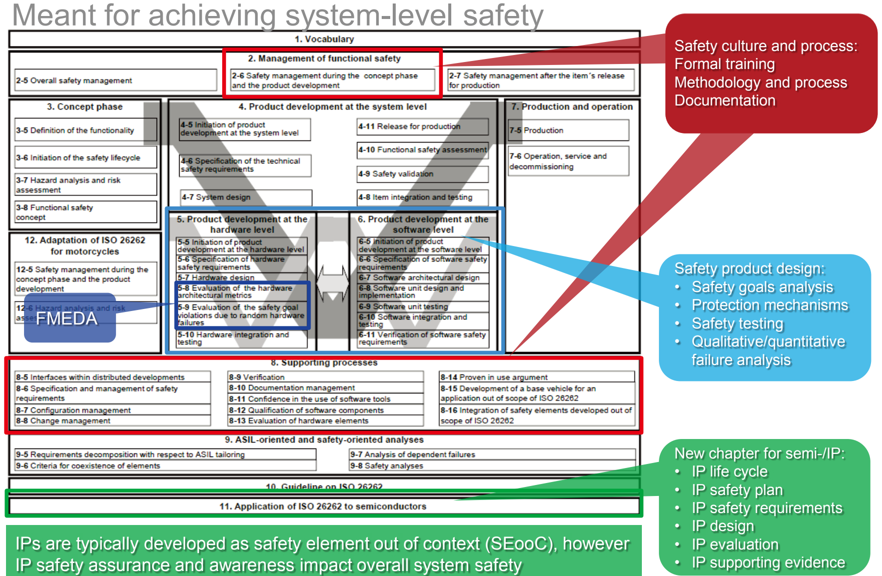
What Can Go Wrong? Failure Modes and Impacts

Where	What's wrong	Impact on System Safety Goals
Local camera/intf	CMOS sensor interface malfunction Image sensing stopped Noisy or distorted image frames Missing pixel/line/frames	Unable to detect road obstacles Unable to detect and recognize traffic signs Unable to detect driving path
Remote camera network	Faulty or interrupted image streams	Unable to detect road obstacles Unable to detect and recognize traffic signs Unable to detect driving path
In-car data network	Faulty communication of data or control	Incorrect or mistimed sensor fusion data or vehicle control data Incorrect or mistimed driving decision
DDR memory	Corruption of memory content	Corruption of code/operation parameters/image data result to incorrect driving decisions
DDR subsystem	Incorrect training or calibration Control state corruption Local buffer corruption Datapath data/address bus error	Corruption of code/operation parameters/image data result to incorrect driving decisions
Data transfer over PCI Express® (PCIe®) for CV processing	PCIe physical link error Incorrect Tx/Rx PCIe transactions Stuck or overflow/underflow Local buffer corruption Datapath data/address bus error	Incorrect or incomplete image data transfer Incorrect or incomplete computation control Incorrect or incomplete computation result transfer Result in false detection/mis-detection or lockup of operations
CV DSP/Hardware	Computation error in ADAS CV DSP processing	false detection/mis-detection or lockup of operations
Real-time CPU	Computation error in processor ADAS driving decision code execution due to processor internal state corruption	Incorrect driving decision Incorrect or untimely control command
Code/data flash	Corruption of ADAS application code or non-volatile data used for ADAS operations (e.g., CNN parameters)	Incorrect driving decision Incorrect or untimely control command Completely lockup or non-operational
Real-time control peripherals	Mal-function of control peripherals	Unable to issue control command Corrupted command/control data or incorrectly target recipient

  cādence

Dissecting ISO 26262: Implications to IPs

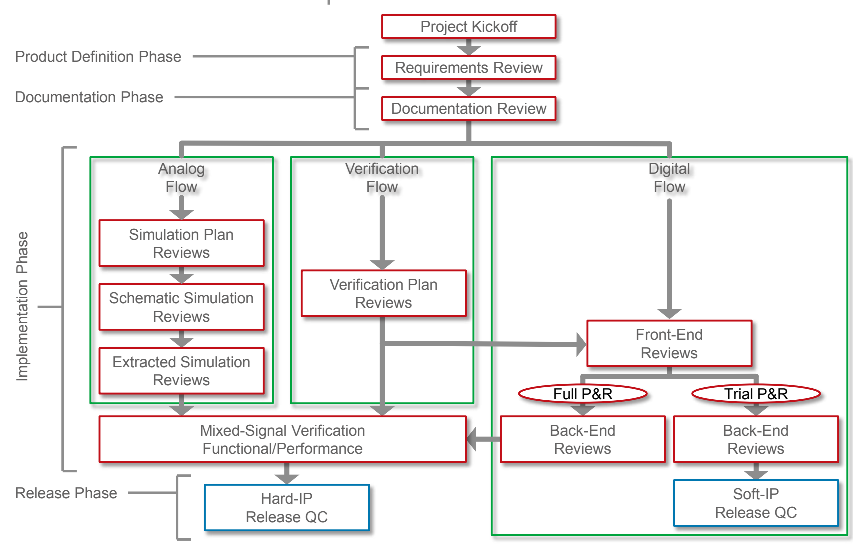
Meant for achieving system-level safety



  cādence

Establish Formal Quality Flow and Checkpoints

Establish baseline QM process



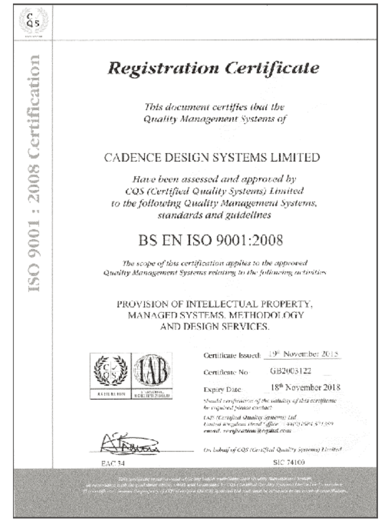
  cādence

Ensure Strict Testing and Release Criteria

Verification Metrics	Target
Regression	
Pass Rate	100%
Stability	5 regression runs in a row with 100% pass
Code Coverage (with waivers)	
Block	100%
Expression	100%
FSM – State	100%
FSM – Transition	100%
Toggle	100% (hierarchical port toggle)
Test Coverage	
Use cases/corner cases/stress cases	100%
Assertion Coverage	
Formal/dynamic assertions	100% (All checkers asserted and passed)
SVA/PSL wreal	100% (for DMS IP only)
Functional Coverage	
Interfaces	100% (UVC functional and checker coverage)
Module/IP features	100% (Functional coverage model for module/IP)
Real value models	100% (Functional coverage of RVM/DMS models)
Release Flow Metrics	**Target**
RTL code quality, LINT, CDC, etc.	No errors and all warnings/waivers reviewed and agreed.
CCD (SDC constraints quality)	No errors and any warnings are peer reviewed and approved prior to release.
RC (Synthesis)	Timing/Power/Area within desired range, log files peer reviewed and approved.
EDI (Place and Route)	Timing/Power/Area within desired range, log files peer reviewed and approved.
LEC (Equivalence Checking)	No errors and any warnings are peer reviewed and approved prior to release.
ATPG (Test coverage quality)	Test coverage figures for soft IP 100%, deviations to be reviewed and approved.
GLS (Gate Level Sims with SDF)	GLS test suite passing at all corners, timing violations reviewed and approved.
Release flow checklist	Review checklist 100% complete, deviations to be reviewed and approved.
GA Checklist Review	**Target**
GA Signoff Checklist review	GA checklist 100% complete, deviations to be reviewed and approved.

Ensure Quality via ISO 9001

Formal site evaluation



ISO 9001 : 2008 Certification

Registration Certificate

This document certifies that the Quality Management Systems of

CADENCE DESIGN SYSTEMS LIMITED

Have been assessed and approved by CQS (Certified Quality Systems) Limited to the following Quality Management Systems, standards and guidelines

BS EN ISO 9001:2008

The scope of this certification applies to the approved Quality Management Systems relating to the following activities

PROVISION OF INTELLECTUAL PROPERTY, MANAGED SYSTEMS, METHODOLOGY AND DESIGN SERVICES.

Certificate Issued: 19th November 2015

Certificate No: GB2003122

Expiry Date: 18th November 2018

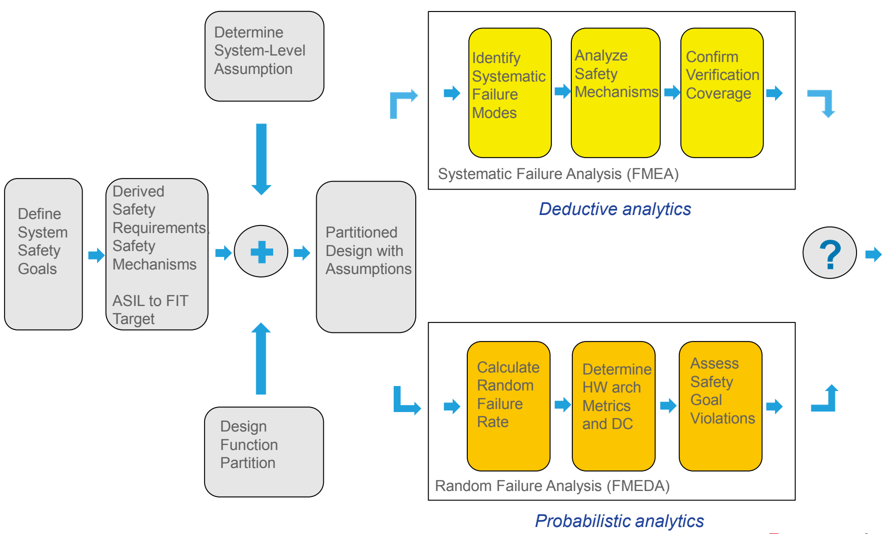
On behalf of CQS (Certified Quality Systems) Limited

EAC 34

SIC 74100

Quantifying Safety by ASIL Levels

Explain the assessment flow linking ASIL levels to failure analysis



A Close Look at FMEDA – Faults and Metrics

Impact of safety mechanism to failure mode classification

Safe fault (λ_S)
→ Fault that leads to a safe condition or has no impact on the respective safety goal

Detected multiple point fault ($\lambda_{MPF\ detected}$)
→ Detected multiple fault
→ No safety goal violation

Perceived multiple point fault ($\lambda_{MPF\ perc.}$)
→ Multiple fault detected by the driver
→ No safety goal violation

Single point fault (λ_{SPF})
→ Undetected single fault
→ Leads to safety goal violation Fault Tolerance Time to be considered

Residual fault (λ_{RF})
→ Partially not detected single fault (due to diagnostic slip)
→ Leads to safety goal violation , Fault Tolerance Time to be considered

Latent multiple point fault ($\lambda_{MPF\ latent}$)
→ Undetected multiple fault
→ Leads to safety goal violation in combination with another independent fault

Faults in logic functions protected by safety mechanism can be re-classed from SPF to MPF

$$\text{Single Point Fault metric} = 1 - \frac{\sum_{\text{Safety related HW elements}} (\lambda_{SPF} + \lambda_{RF})}{\sum_{\text{Safety related HW elements}} \lambda}$$

$$\text{Latent Fault metric} = 1 - \frac{\sum_{\text{safety related HW elements}} (\lambda_{MPF\ Latent})}{\sum_{\text{safety related HW elements}} (\lambda - \lambda_{SPF} - \lambda_{RF})}$$

	ASIL B	ASIL C	ASIL D
Single Point Fault Metric (SPFM)	>= 90%	>= 97%	>=99%
Latent Fault Metric (LFM)	>= 60%	>= 80%	>= 90%

Fault metric targets for latent multi point fault are much lower for ASIL levels

ISO 26262-5, Table 4 + 5

A Close Look at FMEDA – Safety Goal Analysis

Determine probability of failures leading to safety goal violation

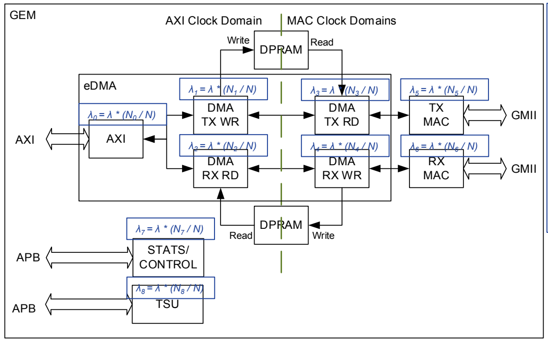
Step 1: nominal IC failure rate calculation according to IEC TR 62380 (2004-08)

MATHEMATICAL MODEL :

$$\lambda = \left\{ \underbrace{\left(\lambda_1 \times N \times e^{-0.35a} + \lambda_2\right) \times \frac{\sum_{i=1}^{y} (\pi_t)_i \times \tau_i}{\tau_{on} + \tau_{off}}}_{\lambda_{die}} + \underbrace{\left\{ 2.75 \times 10^{-3} \times \pi_a \times \left(\sum_{i=1}^{z} (\pi_n)_i \times (\Delta T_i)^{0.68} \right) \times \lambda_3 \right\}}_{\lambda_{package}} + \underbrace{\left\{ \pi_I \times \lambda_{EOS} \right\}}_{\lambda_{overstress}} \right\} \times 10^{-9} / h$$

N: total transistor count
a: years in operation
λ1: per transistor failure rate
λ: FIT for entire IP

Step 2: Compute HW fault metric based on failure distribution and diagnostic coverage



Distribute to sub-modules based on gate count
$\lambda_i = \lambda * (N_i / N)$

Compute metrics (SPFM and LFM) based on fault classification and diagnostic coverage for all sub-modules

$\lambda_{i\,RF} = \lambda_{i\,SPF} * (1 - DC_i)$
$\lambda_{i\,MPF\text{-}L} = \lambda_{i\,MPF} * (1 - DC_i)$

Aggregate to get overall metrics number and check against ASIL targets

  cadence

Active Safety Mechanisms Under Consideration

A summary of effective hardware safety mechanisms

Memory Protection	State Protection	Datapath Protection	Communication Protection

• ECC for RAM
  • 1-bit correction
  • 2-bit detection
• Parity for RAM/flash
• Checksum for ROM
	• Parity for CSRs
	• Redundancy for CSRs
	• Redundancy for FSM state encoding
	• Illegal
		• Data bus ECC
		• Data bus parity
		• Address bus parity
		• FIFO overflow underflow
		• Anti-lockup watchdog
			• PHY layer BER checking
			• Error correction coding
			• Link layer CRC/FCS
			• Transaction layer CRC
			• Header CRC/checksum
			• Illegal format detection

BIST • Memory BIST • Logic BIST • PRBS and loopback • Known answer test	**Electrical Reliability** • Analog operating point calibration • BER calibration • Timing calibration and training • Voltage, temperature monitor	**Failure Notification** • Failure notification pin • Failure notification interrupt • Failure status CSR and event logging counters	**Failure Recovery** • SW/HW reset • SW/HW initiated recalibration • Self correction through error correction code • Self correction through

  cadence

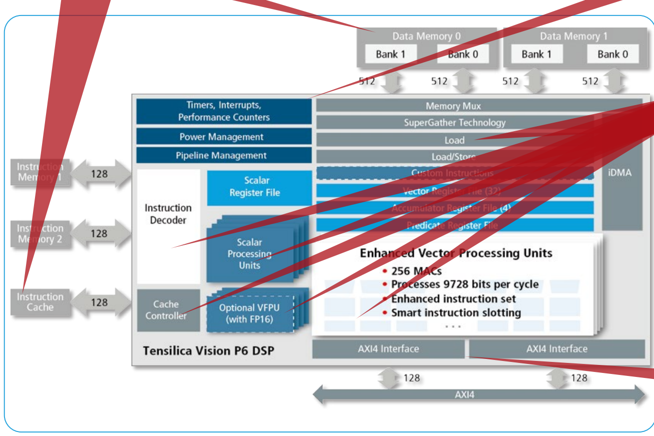
Active Safety Features in Vision DSP Processor

Parity or ECC on cache or local RAMs

High-priority interrupt

Exception handling
- Load/store
- MPU
- Arithmetic
- Program flow

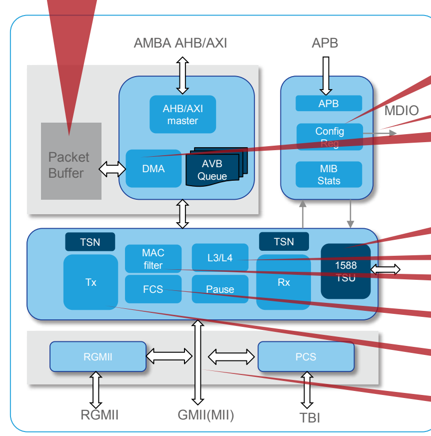
Bus parity or ECC (planned)



  cadence

Active Safety Features in Auto Ethernet MAC IP

Parity or ECC on packet/descriptor buffer



Parity or redundancy of CSRs

Failure status interrupt

DMA descriptor address range checking

Parity protection @ timestamp generation
Redundancy compare

IP/TCP checksum

Illegal packet filter

Ethernet frame FCS

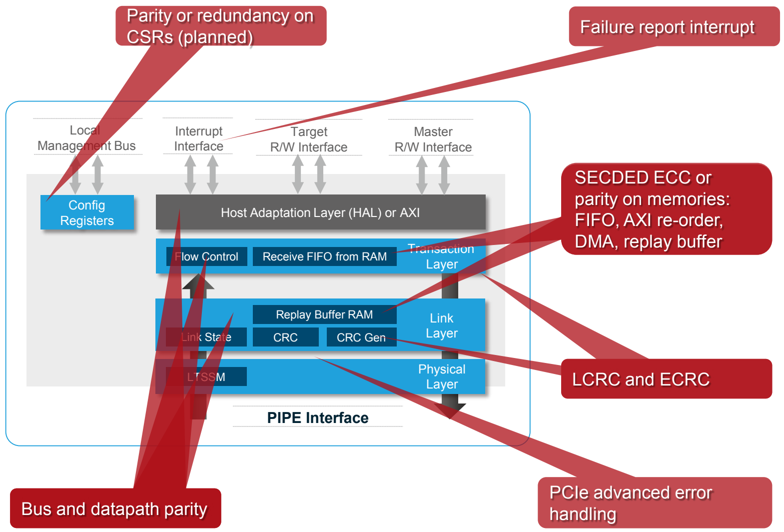
Anti-lockup watchdog

Loopbacks

  cadence

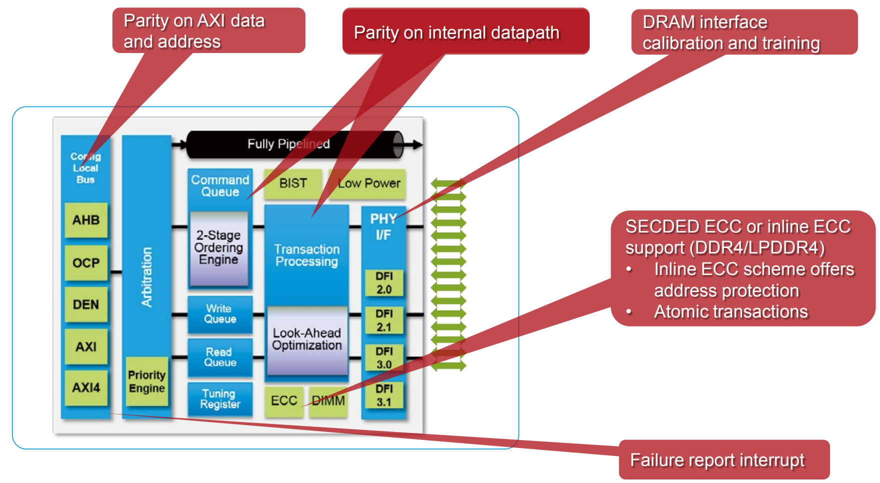
EDA Track
IP Track
EDA / IP / Services Track
Print-Only Papers

Active Safety Features in PCIe Controller IP



cadence

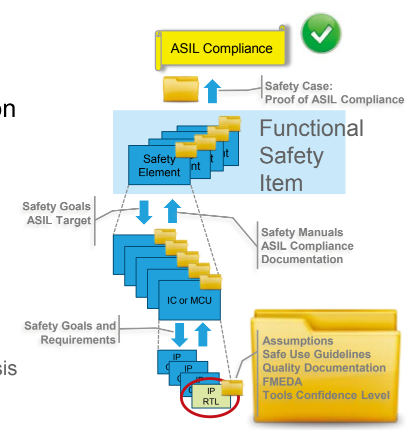
Active Safety Features in DDR Controller IP



cadence

Achieving Proof of Compliance with IP Collaterals

- IPs are developed as SEooC
  - Developed before final requirements are known
  - Evaluation will be to ASIL B level typical
- Cadence provides the documentation needed for our customers (and their customers) to meet their ISO 26262 design targets
- Automotive Safety Integrity Level (ASIL) compliance
  - Quality management process/certification
  - Safety manual for SEooC
  - Safety features description
  - Failure mode effect and diagnostic analysis
  - *Tools confidence level for C compiler (Cadence® Tensilica® DSP)*



cadence

Mitigate Device Failure with AEC-Q100 Qualification

Conducted using IP test chips for hard IPs @ Grade 2

	Standard Requirements	Cadence IP Testing	
Accelerated Life Sim B.ELFR	AEC-Q100-008A • Grade 2: 48 hours at 105°C or 24 hours at 125°C Sample size: 3 lots, 800 parts per lot	Stress temperature: 125° C B-I oven Duration: 2000 hours with 48, 168, 500 and 1000 hour readout Sample size: 80 devices of even mix of 5 corners Test conducted at typical voltage and 125ºC	✓
Accelerated Life Sim B.HTOL	AEC-Q100 Based on JEDEC JESD22-A108 • Grade 2: +105ºC Ta for 1000 hours Sample size: 3 lots, 77 parts per lot		✓
ESD E.HBM	AEC-Q100-002E Based on ANSI/ESDA/JEDEC JS-001 Classification 2 or better Conducted at 500V, 1000V and 2000V	ESD HBM testing conducted according to ANSI/ESDA/JEDEC JS-001-2012 for 4 parts at 2000V	✓
ESD E.CDM	AEC-Q100-011C1 Based on ANSI/ESD S5.3.1-2009, Classification C4B or better Sample size = (# of 250V steps) x 3	ESD CDM testing conducted according to EIA/JESD22-C101_E for 4 parts at +/-600V, +/-650V and +/-750V	✓
Latch-up E.LU	AEC-Q004D Based on JEDEC JESD78 Sample size: 6 parts from 1 lot	conducted according to JESD78 for negative/positive current and over voltage testing on 6 parts	✓
Character-ization E.CHAR	AEC-Q003A provides general guideline that CHAR plan should cover PPM target, corner lots, same sizes, etc.	Multiple skew corners Multiple devices per corner Cold, ambient and hot temperature Supply: (LV, TV, HV)	✓

cadence

Summary

Significantly increased safety requirements on IP
- Complexity of devices in ADAS are increasing
- Customer liability is increasing due to fully autonomous vehicle
- Safety needs to be considered early in IP development

Safety mechanism eases meeting ASIL requirements
- Provides redundancy on failure detection
- Changes failure category from SPF to MPF in FMEDA analysis
- Reduces fault metric target per ASIL level

IP active safety mechanism ensures effective SoC level safety
- Failures can be detected with high coverage and low latency
- Easy to implement localized diagnostics and recovery
- Sensible active safety features in IP reduce SoC level safety design effort